The Thesis Committee for Mohamed Shahid Abdul Ghayum
Certifies that this is the approved version of the following thesis:

Comparative Study of Wireless Protocols - Wi-Fi, Bluetooth, ZigBee, WirelessHART and ISA SP100, and their Effectiveness in Industrial Automation

APPROVED BY
SUPERVISING COMMITTEE:

Supervisor: _____
Aloysius K. Mok

Co-Supervisor: _____
Robert H. Flake

Comparative Study of Wireless Protocols - Wi-Fi, Bluetooth, ZigBee, WirelessHART and ISA SP100, and their Effectiveness in Industrial Automation

by

Mohamed Shahid Abdul Ghayum, B.E.

Thesis

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Science in Engineering

The University of Texas at Austin

December 2010

Dedicated to my family and friends.

Acknowledgements

I would like to thank Dr. Aloysius K. Mok for his valuable guidance, encouragement and support all through this research and the writing process. I attribute the nurturing of my research interest and initiation of my insightful understanding of the subject to him. He has been an excellent mentor, an exceptional teacher and a friendly supervisor.

This research would not have been possible without the help and suggestions from Dr. Robert H. Flake. I highly regard him for his stupendous knowledge and criticisms, and he has been a constant support and guidance since the start of my graduate studies.

Also, I owe my deepest gratitude to Dr. M.A. Khan and Dr. Mary Lourde of Birla Institute of Technology and Science, Pilani – Dubai Campus, in encouraging me to pursue Master's and laying the foundation of this thesis in my undergraduate studies.

Special thanks to all my friends at The University of Texas at Austin including Ninad Patwardhan, Ela Joag, and Munira Rashid who have been a great source of knowledge. I would also like to acknowledge the continued support from friends, Abubakar, Adil, Azhar, Rizwan, and Yasin who have always encouraged me and kept me in high spirits.

Lastly, I owe my deepest gratitude towards, my parents for their eternal love and support. It is because of all of you that I have been able to pursue my goals.

December 2010

Abstract

Comparative Study of Wireless Protocols - Wi-Fi, Bluetooth, ZigBee, WirelessHART and ISA SP100, and their Effectiveness in Industrial Automation

Mohamed Shahid Abdul Ghayum, M.S.E

The University of Texas at Austin, 2010

Supervisors: Aloysius K. Mok, Robert H. Flake

A decade ago, wireless technology was unimaginable in its application in industrial automation as wireless had poor reliability and security in the form of time delays and frame losses. Also, lack of interoperability and standards has been a barrier for wireless applications in control system. But with recent advancements in wireless technology, and with the underlying advantages of wireless like low infrastructural costs, scalability, mobility, and ability to operate in extreme and remote environments, many are seriously considering wireless for industrial automation solutions.

For wireless implementation in industries, it is important to understand its characteristics - security, update rates, data types, protocols, and latency time. Protocol being an important characteristic of any communication, is to be chosen intelligently for

maximum efficiency. Because of the complexity of creating a communication protocol, existing information technology (IT) protocols such as Wi-Fi, Bluetooth, and ZigBee were used in industries. But as applications widened, and interoperability became an important factor to be considered, it was required to standardize the protocols used. ISA SP100 and WirelessHART are results of this standardizing process.

For the last few years, there has been a huge discussion on which of these protocols are robust and work better, and none has emerged as clear winners. The aim of this thesis is to explore the capabilities and limitations of each of these protocols for various industrial applications. This thesis considers all these protocols and helps choose the best fit for industrial applications and includes study of security, reliability, and efficiency of these protocols.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Control System is important and ubiquitous in chemical and pharmaceutical plants, refineries, oil and gas rigs, manufacturing industries and many others where the processes are critical and even a slight mishap would lead to disasters – loss of lives, properties and environmental pollution. Measurement and control forms an essential part of such critical automation systems, as it is responsible for sensing and controlling the process. It involves the measurement of physical parameters like pressure, temperature, level, flow, density, viscosity, current, voltage, frequency, etc. or chemical parameters like composition, properties, etc. The measured value is then compared with the required value of these parameters, and if there is a difference, suitable control action is taken, so as to bring the measure parameter to the required value.

Traditionally, the measurement and control are wired, requiring huge infrastructural support in the form of cables, cable ducts and trays, and power. This generally requires a large monetary investment, and also hampers the dynamic growth of such control systems - scalability.

The revolution in wireless technology with increased robustness, reliability and security, provides low-power and low-cost measurement and control alternatives. Also, wireless advantages include remote accessibility, resource and human mobility, easier installation and many others. This chapter introduces the concept of control system and wireless and ways they could be integrated.

1.1 DISTRIBUTED CONTROL SYSTEMS

Distributed control system (DCS) is a type of control system in which a controller or computer will be distributed to each process separately and each process is connected to a centralized controller (see Figure 1.1). Unlike direct digital control (DDC), controller elements are not in central location (like a brain) but rather distributed throughout the system. The control is partially distributed to few control cards, still in control room, each having several loops.

DCS is different from the more versatile Foundation Fieldbus in a way that the controllers are totally distributed to the field and there is no hard-time control at the control room. Control room merely acts a place of monitoring and taking few control actions.

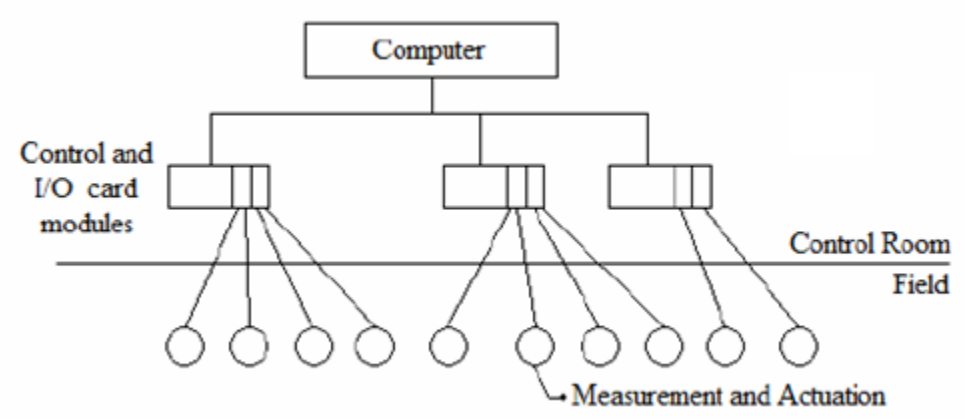

Figure 1.1: Distributed Control System

In general, DCS uses a computer which is usually a custom designed processors or a Programmable Logic Controller (PLC) as controller. It has modular construction i.e. it has input/output modules in which input is fed from the field instruments, a processor

processes the data and transmits this information to the main or central computer or controller using the output module. And during a control action, the input module receives the control signal from the central controller and output is sent to actuators in the field and once again the processor acts as the mediator. Typically, the connection between the transmitters at the field and the control I/O cards at the control room and within the control room are hard-wired buses.

DCS is an advanced version of DDC and the advantage of DCS over its counterparts is that there is an increased availability of microprocessors for each process making the process more resourceful.

1.1 Architecture of DCS

The architecture of the Distributed Control System is explained with the help of the schematic diagram (Figure 1.2) [1]:

1) Local Control Unit (LCU): LCU is the smallest collection of hardware in the system that can do a closed loop control. It is one of the few sub-systems that interface directly with the process.
2) Low Level Human Interface (LLHI): LLHI is an operator-oriented hardware device that allows the operator or an instrument engineer to interact with the LCU. Example: Changing the set-point, control modes, control configurations, tuning parameters etc. This sub-system also interfaces with the process through LCU. Operator interface at this level is called Low Level Operator Interface.

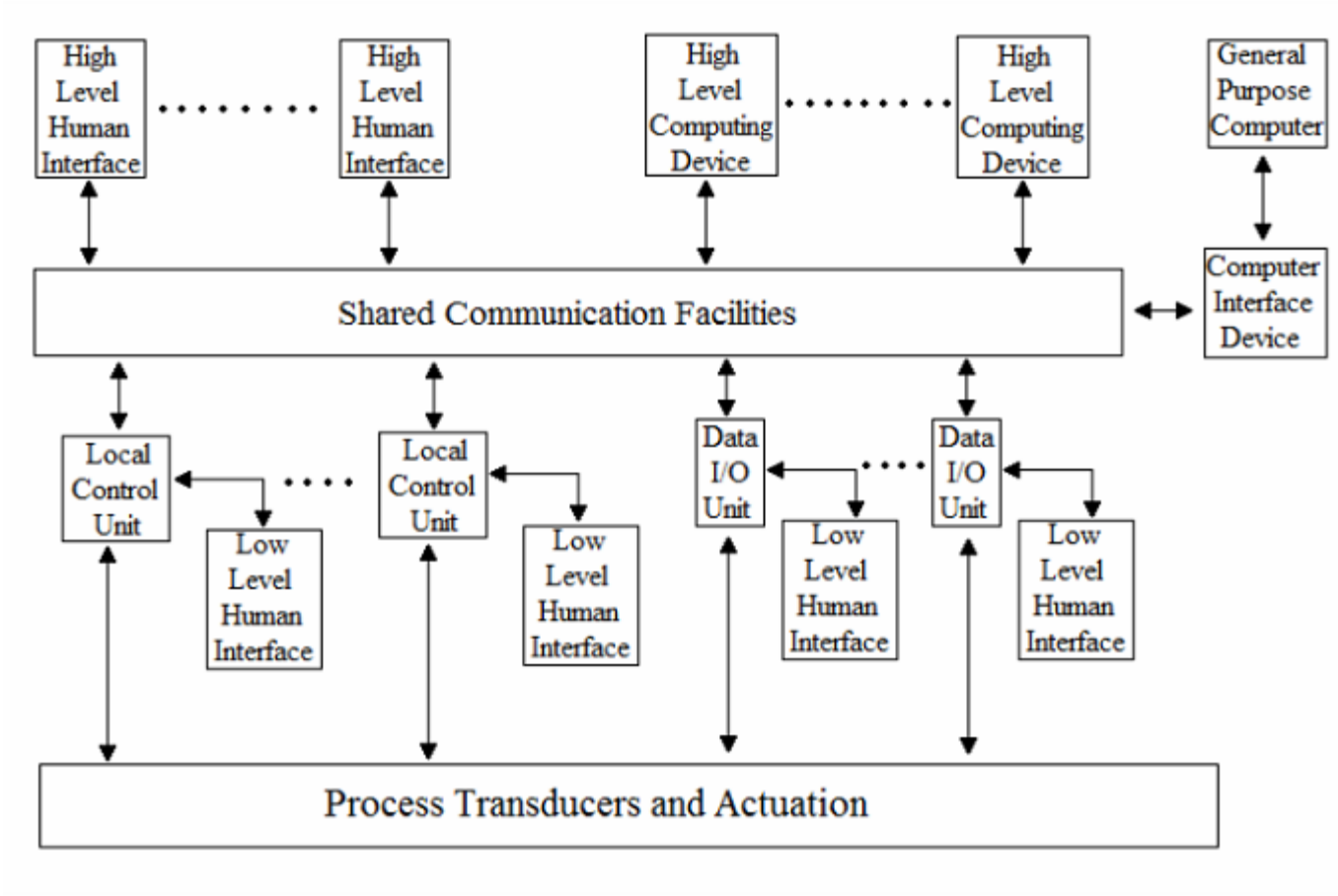

Figure 1.2: DCS Architecture

3) Data Input / Output Unit (DI/OU): DI/OU is a device that interfaces to the process solely for the purpose of acquiring or output data. This sub-system performs no control action.
4) High Level Human Interface (HLHI): HLHI is a collection of hardware that performs functions similar to LLHI but with increased capability and user friendliness. It interfaces with other devices only over the shared communication facilities. Operator oriented hardware at this level is called High Level Operator interface.
5) High Level Computing Device (HLCD): A collection of microprocessors based hardware that performs plant management functions is called HLCD. It interfaces with other devices only over the shared communication facilities.
6) Computer Interface Device (CID): A collection of hardware that allows an external general purpose computer to interact with other devices in DCS using shared communications facilities is called CID.
7) Shared Communication Facilities: Shared Communication Facility is one or more levels of communication hardware and associated software that allow sharing of data among all devices in the DCS. It does not have dedicated communication channels between devices or hardware elements.

1.2 Features of DCS

There are a number of features of DCS that makes it to stand-out among other control techniques – DDC and Foundation Fieldbus and most distinctive ones are listed below [1]:

1) Scalability and Expandability: DCS can be sized for a spectrum of applications ranging from small to ultra large processes. Elements can be added to the system after initial installation. Scalability and expandability offers good modularity which is the key aspect of DCS.
2) Control Capability: Full digital control offers drift less set point and tuning parameters, availability of complex control algorithms, ability to change an algorithm without changing the hardware and remote tuning capabilities.
3) Operator Interface Capability: Two levels of operator interface are provided with DCS and this offers higher operability and user friendliness.
4) Integration of System Functions: Various functions are integrated in a family of products. It also refers to the degree with which the various functional sub-systems are designed to work with one another in an integrated fashion. High degree of integration minimizes user problem in interfacing, start up and maintenance.
5) Significance of Single Point Failure: Single point failure is low due to modularity and as a result of usage redundant devices.
6) Installation Costs: Cost is low because of savings in both wiring costs and equipment space. Also because of the shared communication cost is reduced considerably. Due to the microprocessor based module the equipment space is also greatly minimized.
7) Maintainability: Maintainability is excellent as DCS has automatics diagnostic and module replacement systems. These systems isolate the failures to the module level and replace it without disrupting a major portion of the process.

1.2 WIRELESS IN DCS

Wireless is just another physical media for process data transmission instead of wires in a DCS and there can be a number of ways wireless can be employed in the automation of industries. As it can be seen from the below Figure 1.3, there are three levels of networks in any DCS. [2]

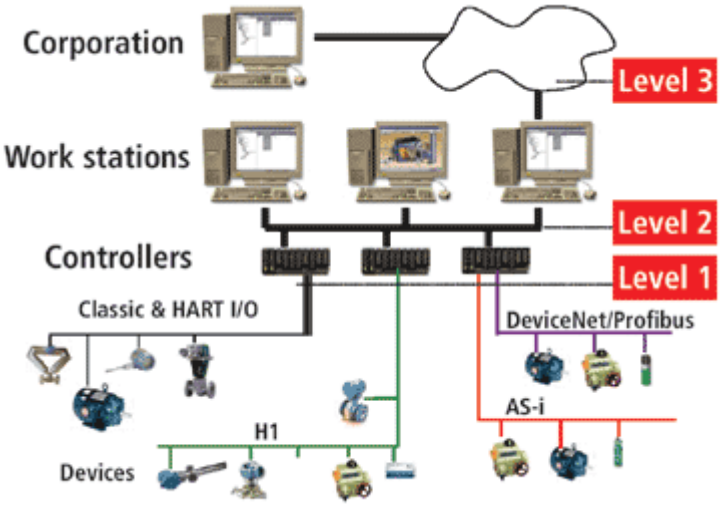

Figure 1.3: Different levels of DCS [2]

Wireless can be implemented in the DCS in any of the three ways corresponding to three layers of DCS:

1) Level 1: The hard-wires from field instruments to the control modules / controllers and back to the actuators in the field can be replaced with wireless. This involves radio integration at the instruments, actuators and controllers.
2) Level 2: The other way of inducing wireless in the DCS is by replacing the traditionally hard-wired between the various controllers and the workstations

or the SCADA system involving wireless integration at the controllers and workstations.

3) Level 3: Lastly, corporation can be connected to the workstations through wireless.

The heart of the process resides at the Level one of the DCS tree. Transmission at this level is highly real-time and should be highly deterministic and reliable. The sensor-receiver distance is within few hundred feet and data sizes are very small. WirelessHART, ISA SP100.11a, ZigBee, and Bluetooth are some protocols that find usage for this requirement.

One level up the tree connects various control modules to the workstation that provides operator interaction and device configuration of the field devices. In the wired world, Ethernet or proprietary protocols is used at this level which can be replaced by Wi-Fi. Non-process control entities such as accounting, inventory, and management decision systems access the workstations for data collection and analysis. This requires lesser complexities in switching from wired to wireless than levels one and two. [2]

Wireless technology when integrated into DCS provides more flexibility than the traditional wired DCS. In addition to asset management, maintenance, and trouble-shooting, wireless field instruments and actuators can also provide reliable closed-loop control.

1.3 RESEARCH OBJECTIVES AND OVERVIEW OF THESIS

The aim of this research is to explore the capabilities and limitations of various industrial wireless standard protocols vis-à-vis WirelessHART, ISA SP100.11a, ZigBee,

Bluetooth and Wi-Fi in their application in industrial automation. The project involves extensive study on wireless as an technology, followed by technical study on different wireless protocols available for industrial automation and compare them for their robustness, reliability and interoperability for industrial control applications – both monitoring and control.

The sections discussed earlier 1.1-1.2 gave a brief introduction of distributed control systems and the levels where wireless can be employed. Chapter 2 discusses in detail the wireless technology – wireless myths, inherent features such as signal losses and multipath fading, characteristics, advantages, and factors to consider for wireless implementation in DCS.

Chapter 3 discusses the technical specifications of the different industry standard protocols available which can be broadly classified as IEEE 802.11, IEEE 802.15.1 and IEEE 802.15.4 based protocols. After exploring their specifications, Chapter 4 draws a comparison of the different protocols available for industry automation in two categories: Specifications-based and Applications-based. The former compares the protocols on the inherent specifications while the later tailors the protocols according to the applications it would be installed in. Four detailed practical cases are chosen in which the applicability of different protocols is illustrated. Finally, Chapter 5 concludes with the key findings of this research and suggests a direction for the future work.

Chapter 2

Wireless – A Detailed Study

Traditionally, wireless was employed to communicate over long distances through satellites, transmission towers, and big antennae for uses in telecommunications, televisions, radios and military purposes. But along the years, wireless has become an all-encompassing technology and has found usage in everyday life from Wi-Fi in laptops, Bluetooth in cell phones, among many others. Few years ago, no one dared to dream of wireless technology's application in control system, as it had long time delays, frame losses and poor security, to name a few, all causes of major calamity in any control system environment [3]. But with advances in wireless technology recently, wireless has found application in monitoring and control in factory and plant automation. Now, wireless is no longer restricted for long communication distances but also employed within areas of 100 feet diameter or even lesser.

2.1 WIRELESS MYTHS

At the end of last century, wireless found use in plant automation in transmitting process variables over long distances using the Remote Terminal Units (RTUs), that used the Industrial, Scientific, and Medical (ISM) 900MHz band. But it was never thought of as a technology that could potentially replace hard-wires that ran from instruments to the control room. This was always unthinkable and hesitated, because of the reluctance to embrace upcoming wireless advancements and fear of disasters at the plants or factories

which could potentially cost lives and equipments losses. There were a large number of pre-conceived notions about wireless and few of the common wireless myths were [3]:

1) Data transfer delays: The processes or manufacturing in the plant or factory are highly time critical, and there needs to be minimal latency in the ranges of milliseconds for the measured variable to be read by the controller and the control action has to be sent within the same time period. So, time is major criterion in industrial automation.
2) Communication failures: Since the processes and the manufacturing lines are highly critical and needs the exact information from the measurement units to produce a result, the frame needs to arrive fully with all the data content intact for the right decision to be made. As such frame losses cannot be tolerated for any control system design.
3) Standards: There were no industrially acceptable norms or standards that existed for wireless technology as wired counterparts and the only norm that existed were the government issued rules or procedures for the usage of wireless in their factory settings or environment.
4) Security: No factory or plant want their information to be leaked to any kind of outside intruders, for plant safety as well as for management reasons, as a result security cannot be compromised at any cost.
5) Reliability: The controller does not take an action unless it receives an input from the instrument and the final control element doesn't provide any effect without the signal from the controller. So, the data needs to be transmitted

reliably for any effect to take place. The system becomes more critical in cases of alarms and reliability is an important factor for any communication.

6) Powering Options: As with the law of conservation of energy goes, every device needs an input electrical power for it to operate. Having a power cable connected to the device would solve this problem, but the device may not be completely "wireless". Batteries or other forms of energy (solar) are good alternatives but even then it needs maintenance.
7) Wireless implementation on the plant floor is feared because of the complexity and the integration with the already existing host – backward compatibility. Also, wireless is thought of as pre-natal technology and cannot be incorporated in control, it all implemented for monitoring.

2.2 WIRED VS. WIRELESS

As with any communication media, wireless has inherent losses while being transmitted in the channel. Radio signals propagate as light does and follow a straight path from the sender to the receiver called the line-of-sight (LOS). Even in media with null disturbances such as the vacuum, transmitted signals experience free space loss. This issue becomes more complex as soon as there is any matter between the sender and receiver. Generally, in an industry environment, signals travel through the atmospheric variables such as the air, rain, snow, fog, dust particles, smog, etc and also through the various metal machineries and equipments made of steel and aluminum. These factors greatly influence the transmission so the received power is never equal to the transmitted power and there is always a path loss or attenuation [4].

The mechanisms behind electromagnetic wave propagation are diverse, but can generally be attributed to reflection, diffraction and scattering. These physical phenomena along with refraction and shadowing cause large-scale path loss [5]. Also due to multiple reflections from various obstacles, the electromagnetic waves travel along different paths of varying lengths. The interaction or interference between these waves causes multipath fading and the strength of the waves decrease as the distance between the transmitter and receiver increases [5], [6].

2.2.1 Large-Scale Path Loss

Signal propagation in free space follows a straight line, but in reality there rarely exists a line-of-sight. The received power is proportional to $1/d^2$ where d is the transmitter-receiver distance. In addition to this there are several other frequency-dependant factors that affect the strength of the signals. An extreme form of attenuation is shadowing due to large obstacles [5]. This effect is even more evident if the frequency of transmission is very high. Another effect is the reflection of signals by huge buildings, mountains, ships or even the surface of ground. This effect is more prominent if an object is large as compared to the wavelength of the signal. [4] Most of the propagating wave is reflected by the medium whereas a part of it is transmitted. As the obstructions are not purely reflective medium and absorb a certain amount of energy, the reflected signal is not as powerful as the original LOS signal. The more often the signal gets reflected, the weaker the received signal becomes [4], [6].

The quality of the reflected signal depends on the surface by which it is reflected – dielectric or conductor and the angle of incidence. The velocity of the electromagnetic

wave is different in different mediums, i.e. velocity is dependent on the density of the medium through which it travels. The EM waves bends as they travel from a lighter medium to a denser medium or vice-versa. This effect is called refraction and is reason for the radio waves bent towards the earth [5].

The above discussed physical phenomena vis-à-vis, reflection, shadowing and refraction highlights the particle nature of waves and are caused by objects larger in magnitude than the wavelength. Signals falling on smaller objects undergo scattering and diffraction demonstrating the wave character of signals [5], [6].

Diffraction is the effect in which radio waves will be deflected at an edge and propagate in different directions [5]. Diffraction allows radio signals to propagate beyond the horizon, and to propagate behind obstructions. In the shadowed region, the diffraction field exists and often has sufficient energy to produce useful signal. The phenomenon of diffraction can be explained by Huygen's principle, which states that all points on a wavefront can be considered as point sources for production of secondary wavelets, and these wavelets combine to produce a new wavefront in the direction of propagation. Diffraction occurs when the radio path between transmitter and receiver is obstructed by a surface that has sharp irregularities [5], [6].

The actual received signal in a radio channel is often stronger than what is predicted by reflection and diffraction models alone. This is because when a radio wave impinges on a rough surface, the reflected energy is diffused in all directions due to scattering, thereby providing additional energy at the receiver. An incoming signal is scattered into several weaker outgoing signals.

If the size of an obstacle is in the order of wavelength or less and where the number of obstacles per unit volume is large, the waves can be scattered [6]. Thus many objects in the environment can cause scattering effects. Effects like reflection, shadowing, diffraction and refraction all happens simultaneously and are frequency and time dependant [6]. It is very difficult to predict the precise strength of signals at a certain point in space. Propagation models are developed to predict the mean received signal strength at a given distance from the transmitter.

The below figure illustrates the free space loss in dB at different radio frequencies over distance. It can be easily concluded that free space loss increases with frequency and distance.

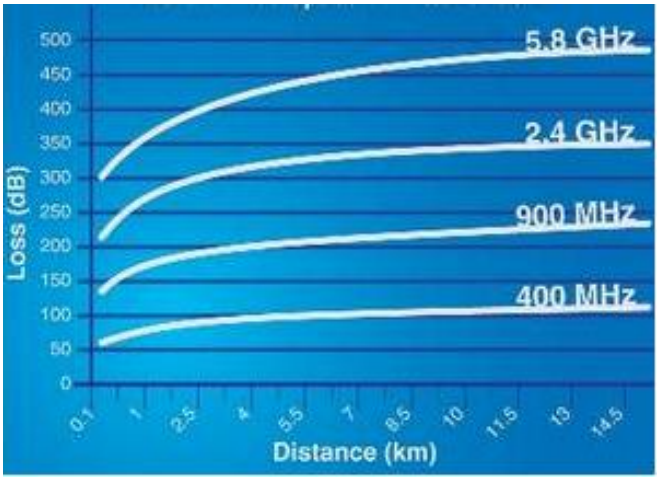

Figure 2.4: Free space loss vs. Distance and Frequency [8]

2.2.2 Multi-path Fading

Together with the direct transmission from a sender to receiver, the propagation effects mentioned in the previous section lead to one of the most severe radio channel impairments, called multi-path propagation [4]. Fading is due to rapid fluctuations of the amplitudes, phases, or multipath delays of a received signal over a short period of time [5]. This is caused by interference between two or more versions of the transmitted signal which arrive at the receiver at slightly different times. Radio waves emitted by the sender can either travel along a straight line, or they may be reflected at a large building, or scattered at smaller obstacles. In reality, many paths are possible.

Due to the finite speed of light, signals traveling along different paths with different lengths arrive at the receiver at different times. This effect (caused by multi-path propagation) is called delay spread: the original signal is spread due to different delays of parts of the signal. In addition to a LOS, multipath occurs due to reflections from ground and surrounding structures. These multipath components combine vectorially at the receiver antenna, and cause the signal received to fade or distort. The first effect is that a short impulse will be smeared out into a broader impulse, or rather into several weaker impulses [6].

These waves, called multipath waves, combine at the receiver antenna to give a resultant signal which can vary widely in amplitude and phase, depending on the distribution of the intensity and relative propagation time of waves and bandwidth of the transmitted signal [5]. Even when there is no relative motion between the transmitter and receiver, the signal may fade due to movement of surrounding objects.

Due to the spreading of the transmitted signal at the receiver end, the energy intended for one symbol now spills over to the adjacent symbol, an effect which is called inter-symbol interference (ISI) [5]. The higher the symbol rate to be transmitted, the worse the effects of ISI will be, as the original symbols are moved closer and closer to each other. ISI limits the bandwidth of a radio channel with multi-path propagation (which is the standard case). Due to this interference, the signals of different symbols can cancel each other out leading to misinterpretations at the receiver and causing transmission errors [5].

2.2.3 Shared Airwaves

As with wired world where there can be no more that few wires that bundled in a cable conduit, the air space is also limited for wireless technology. Government agencies around the globe allocate frequency band to be used for telecommunication (television, public radio, cell phones), industrial, commercial and military purposes. The allocation of the air space is highly dependent on the technological advancements and economic conditions and as such there are shared bandwidth and unshared bandwidth. As the name signifies unshared bandwidth cannot be shared and are reserved for particular applications. Examples of unshared bandwidth usage include military, radio, television, GPS, etc. Of the limited shared bandwidth available for industrial and commercial usage, it can be broadly classified as licensed and unlicensed.

Licensed bands, generally, transmits higher power for longer distances, while the unlicensed bands are mainly for short distance applications [9]. Most of the plant or factory automations uses this short distance unlicensed bands. Although there is a huge

constraint on bandwidth and many applications fight for their share of air space, technological advancements have made possible sharing of this limited resource in an efficient way for better functionality of the systems. Techniques such as multiple accessing, delay of transmission and broadcasting the information on frequency usage and duty cycles on cluttered networks pave way to better utilize the shared air waves [9].

In the United States, there are three license-free frequency bands that can be used: 900 MHz, 2.4 GHz, and 5 GHz, commonly called the ISM (industrial, scientific, and medical) bands.

2.3 ANTENNA

The choice of antenna is an important factor for any wireless communication that cannot be compromised. An antenna is the final device in the transmission and the first device at the reception end. It is a transducer that converts electric current to e-m radiation during transmission and converts e-m radiation to the current at reception. The design antennas depend on antenna parameters such as the gain, polarization, bandwidth, aperture, radiation patterns, among many others that affect the performance of an antenna [7], [9].

Antenna size is directly related to the wavelength of the signal it transmits. With the increasing frequencies or the reducing wavelength, the antenna sizes have reduced considerably. The full-length antenna sizing can be easily computed by: wavelength(m) = $3 \times 10^8 \div$ frequency(Hz), although ½ wavelength or ¼ wavelength antennas are normally used [9].

The sensitivity of the radio is also a governing factor for a good radio communication. The mathematical expression for successful radio reception is [7]:

(TX power + TX antenna gain - Path loss -

Cabling loss + RX antenna gain – 10dB > RX radio sensitivity or RF noise floor fade margin)

There are various kinds of antennas that are available for use and mainly depend on the application and environment. The two important and relevant ones are discussed below [9]:

1) Omni-directional: As the name signifies the radiated wave from this antenna travel in all directions. This is particularly useful in mesh networking where there are a number of hops between the end devices and gateway that connects to the control system.
2) High-Gain Directional: The transmitting antenna transmits the signal in a single direction and the received signal is concentrated by the receiving antenna to improve the gain. Such an antenna is useful where channel losses are high and directional antennas also improves security.

2.4 WIRELESS CHARACTERISTICS

To understand the working of wireless in the industrial environment it is important to know the features required of wireless equipments. The following details the characteristics:

2.4.1 Communication Protocols

A protocol is defined as the collection of rules or conventions for data communication. It features the procedures for data representation, signaling, authentication and error detection required to send information over a communication channel [10]. At the beginning of the wireless implementation in industrial automation it was easier to use the existing information technology protocols, but as applications increased the need for a standard industrial wireless protocol grew. The use of one or the other protocol is governed by the application it is used for and the capabilities and limitations of each protocol.

The different protocols available are: Bluetooth (IEEE 802.15.1) – Low power, short range, medium data rates, ZigBee (IEEE 802.15.4) – Ultra low power, larger scale networks, low data rates, WiFi (IEEE 802.11b) – High rate data transfer, higher power, WirelessHART, and ISA SP100.11a.

2.4.2 Security

As mentioned earlier in the Wireless Myths section, there is a high importance given to the security measures in wireless deployments in industrial environment. There are many ways to protect the intrusion of foreign invasion of the network. On the hardware side, highly directional antennas can be used to protect the network by only having a LOS between the transmitter and the receiver, thereby preventing others to intervene the radiated the signals.

Security can be increased on the software side by using encryption techniques. There are a number of encryption methods available that uses either a secret key or

private/public key. The data is encrypted using an unique key and the received data can only be read with the same key. The secret key is used in Data Encryption Standard (DES-64) and Advanced Encryption Standard (AES-128 or AES-256) algorithms. As far as the use of public/private key encryption methods: RSA (Rivest-Shamir-Adleman), and PGP (Pretty Good Privacy) are widely used and provides better encryption techniques [9].

2.4.3 Update rates

Update rate is defined as the frequency in which the data is to be sent to the control system for any control action. Most applications do not require the sending of information continuously needed for critical operations. Update rate is an important factor to consider since it is directly proportional to the battery life of the equipment. The more frequent the device is involved in transmitting data, the more power it consumes and lessens the battery life. Also, update rates puts a limit on the number of devices that can be connected to the gateway [11]. The more the update rate the lesser the devices that can be connected to the given gateway, because the gateway would be busy serving this fast-updating device. Generally, update rate of 1 minute 1500 devices can be connected to a gateway and for 1 second the devices is reduced to 30.

As a result, the update rate should not be any longer than what the process requires. As an alternative, there is option of the use of alerting functions, in which the device transmits only if it is required to do so, as in the case of alarms thus saving a significant amount of power.

2.4.4 Data types and data rates

Data types transmitted by the instruments for the process variable can range between a byte to a complex waveform and as such the transmission times will also differ for each of the transmitters. Bytes can be transmitted with short bursts of data and time required increases with the complexity of the data type [11].

When a data is transmitted over the air, it is sent over a frequency band that has many channels. This is called channel bandwidth and is measured in bytes per second, normally kilobytes and megabytes. For higher-speed transmission we would require a wide bandwidth, thus increasing the amount of interference. Also, higher-speed radio decreases the energy per bit thus having a limiting factor on the transmission distance. Thus, to obtain a long range and less interference, it is apt to lesser transmission speeds.

2.4.5 Power

As per the law of conservation of energy, every device requires power to operate itself. Power can be fed in to a wireless instrument through: Batteries, Power source located near the instrument, or alternate sources of power such as the solar energy. The choice is totally dependent on the application served and availability of power. When there is a static instrument installed near a power source, getting rid of the data cable is good option and it is sensible to use that capability. Devices that require higher power such as flow meters may have external power source fed through a cable. In a place, where solar energy can be harnessed, having solar cells would be a better idea to power the equipment. But in 80% of the applications batteries are the norm for power source.

2.4.6 Latency

The delay in getting information packet from its source to its destination is called latency. The objective of any wireless system is to maximize determinism i.e. to get the information as quick as possible with minimum errors and minimize latency. Latency is also affected by the number of hops the data makes when sent form source to the destination, the more the number of hops the more the latency.

2.4.7 Transmission methods

Transmission methods [8] are unique ways of transporting data in the air for various ranges of distances. The ones used for wireless industrial automation include, fixed frequency, Frequency-hopping spread spectrum (FHSS), Direct-sequence spread spectrum (DSSS), and Orthogonal frequency-division multiplexing (OFDM). The below figure illustrates these transmission methods.

In fixed frequency method, high-power signals are transmitted over single frequency over time. In Frequency Hopping Spread Spectrum (FHSS), the radio signals are switched over different frequencies in the channel bandwidth using a pseudorandom sequence. The receiver uses the same pseudorandom sequence used for transmission to retrieve the data. In Direct Sequence Spread Spectrum (DSSS), frequencies of the signals are spread over the channel bandwidth using spreading algorithms. Reversing the algorithm retrieves the information thus minimizing interference and signal-to-noise ratio. In Orthogonal Frequency Division Multiplexing (OFDM), a signal is transmitted on multiple frequencies at one instant of a time thereby increasing data rates.

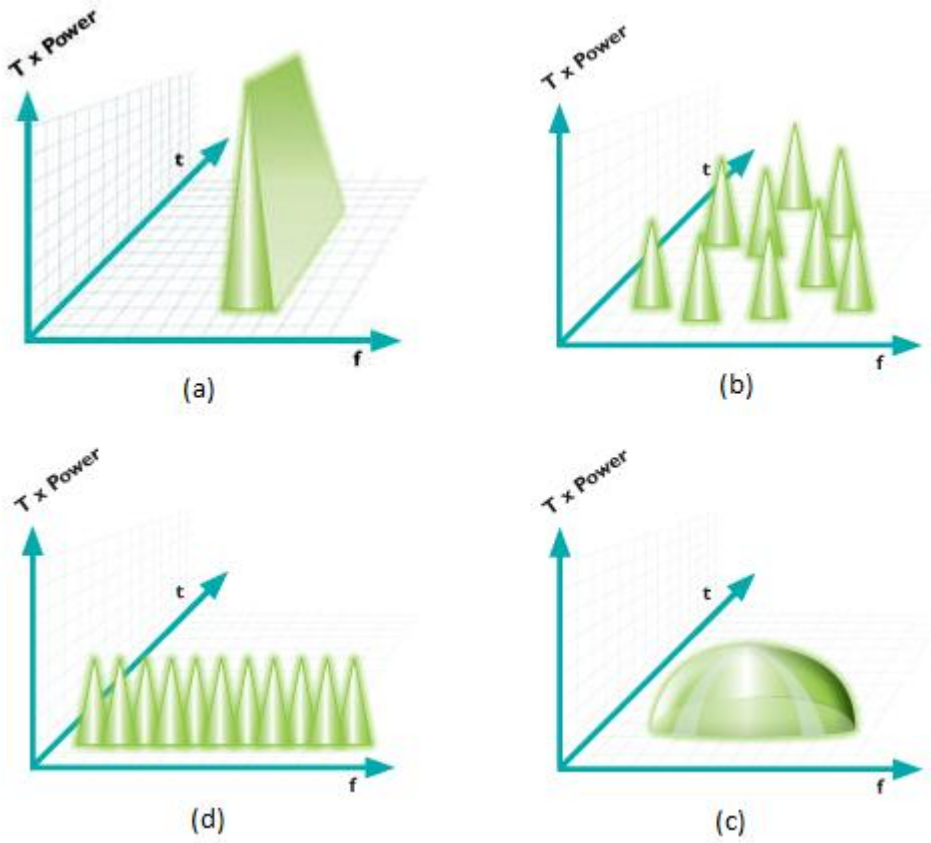

Figure 2.5: Transmission methods: (a) Fixed Frequency (b) Frequency Hopping Spread Spectrum, FHSS (c) Direct Sequence Spread Spectrum, DSSS and (d) Orthogonal Frequency Division Multiplexing, OFDM [8]

2.4.8 Network Membership

Wireless instruments are added to the network by the gateway as soon as the power is on the devices. When the instruments join the network they are assigned a unique network address that is used to communicate with the network. This network key or address is used each time for data transmission, so as the gateway realizes it is from its network which also adds a layer of security [9].

2.4.9 Radio Configuration

The antenna or the radio can be either built-in with the electronics of the instrument or can be a separate module that is attached to the instrument. The choice resides on the powering issues again, and instruments that do not require much power can have integrated radio. But devices that consume a lot of power such as flow meters have externally powered radio module that is attached with instrument [11].

2.5 WIRELESS TOPOLOGIES

There are various ways a network can be set-up for the devices in the network to communicate, but in the field of plant or factory automation the following topologies are used [11]:

2.5.1 Point-to-point and Star

The most basic topology of a wireless set-up is point-to-point, in which there is one instrument-gateway pair. A gateway is nothing but a receiver and is wired to the control system. This is suitable for processes having smaller number of instruments but for larger networks this approach is not viable as the infrastructural costs increases and also the probability of interference between different systems also increases.

In star topology a set of transmitters independently send their signals wirelessly to one receiver that is connected to the control system. But this adds burden to the gateway as it has to sort out the data sent from different radios at different times.

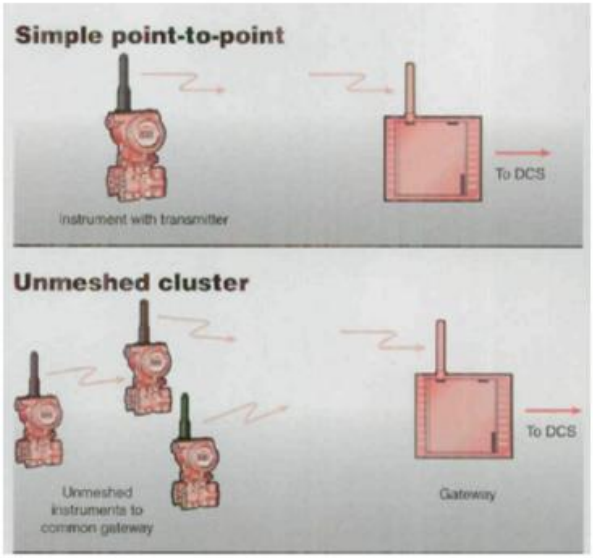

Figure 2.6: Point-to-point and Star Topology [11]

Data concentrators are externally powered nodes that transmit data to the gateway. These are less widely used topology on Wireless Fieldbus with two variations: Fieldbus segment Hub transmitter and Segment Hub and gateway.

2.5.2 Mesh networks

There are two main methodologies: meshed instrument network and meshed node network. The first approach is fully dependent on battery powered individual instruments. Each device is a transceiver, and devices that are within range of each other communicate with each other and the gateway. There is a lot of time delay and battery consumption in this methodology.

The other approach is meshed node network. There are externally powered nodes that mesh with each other and thereby save the battery power of the instruments.

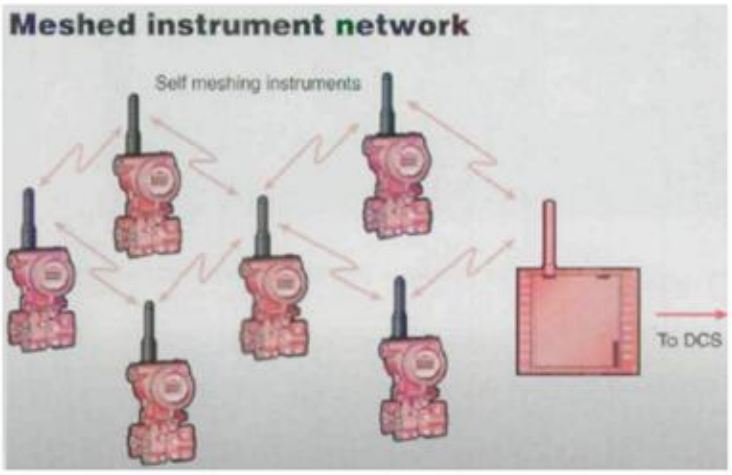

Figure 2.4: Meshed instrument network [11]

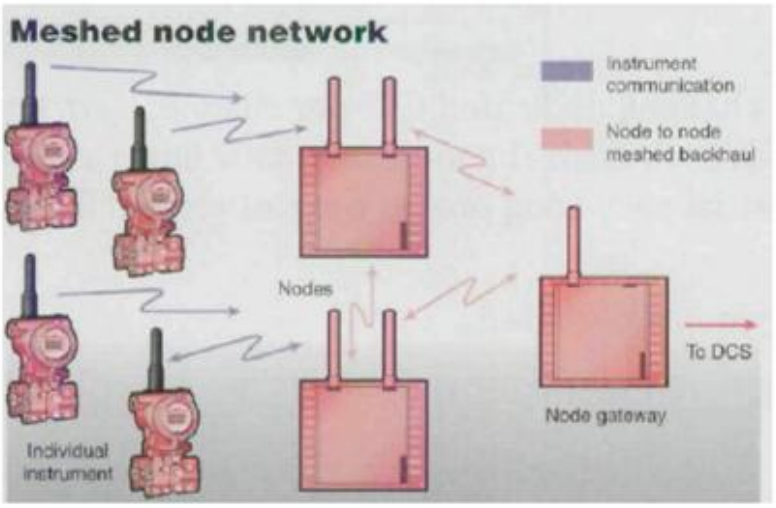

Figure 2.5: Meshed Node Network [11]

2.6 ADVANTAGES OF WIRELESS

With the advancements in the wireless technology in the last two decades, wireless have become secure, reliable, robust, thus encompassing all walks of life. It is

only a matter of time that the industrial automation field embraces wireless because of various advantages it posses.

The following details the advantages:

1) Low cabling and infrastructural costs: In a typical control system, instruments are wired to the control room, using cables, cable ducts, cable conduits, cable trays, connectors, termination and marshalling boxes and other infrastructure that can be completely eliminated by wireless. Accordingly over 90% of the cost can be recovered by using a wireless instrument. Also, many of the downtimes in the factory set-up can be attributed to the cable malfunction, and by removing cables these downtimes can be avoided successfully.
2) Scalability: The ability of the system to dynamically grow without much infrastructural change is possible using wireless. In wired world, to add an measurement point, cables have to be run from the control room all the way to the instrument, but with wireless growing the network is as simple as turning on the device and configuring the control room applications.
3) Mobility: With wireless, mobility of the instrument can be achieved without tangling of wires, for example in a rotating kiln in a cement plant, the kiln rotates twice per minute and using a wired solution is impossible to measure the process variable in this application. Also, mobility can be achieved at the human-level, and the workers can use their hand-held wireless enabled Personal Digital Assistants (PDAs) to oversee a part of plant or factory. This would also ensure safety of the workers in an harsh environment by reducing operator rounds.

4) Ability to operate in varied environment: Few measurements are desired from places from the environment doesn't really provide the ability to run a wire such as corrosive environments, chemical or bio-hazard plants. The ability of wireless to operate in such environments provides immense advantage at these sites.
5) Remote applications: Measurements from long distances cannot be obtained practically by laying a cable for miles. In such scenarios, wireless is the most optimal solution providing greater visibility and reduced operator rounds
6) Plant optimization: Many variables that were untapped at the instrument in the wired world can now be obtained easily using a wireless adaptor. Also additional measurement points can be added easily thereby increasing plant operational productivity. It also simplifies management with better data integration.
7) Quick installation time: Since setting up a wireless network doesn't require as much resource as wire, it is quicker to install and helps in the fast completion of the project, thereby decreasing the run-time.

With these advantages many factories and plants are seriously considering wireless technology as their industrial automation solution.

2.7 SUMMARY

This chapter introduced the technology of wireless and discussed about the inherent characteristics of radio communication and wireless solutions. In addition, it jolts down the fundamental principles of wireless communication to pave way to clear

many of the misconceptions about the wireless and highlight the benefits of wireless on the plant and factory floors.

This chapter also laid foundation to understand the applications that dictate the implementation of wireless and to understand the differences in the available technologies. After studying the details of the wireless technology and the advantages of it, the next step is to choose the best fit standard for a wireless application. Large number of factors is to be kept in mind, when choosing a wireless solution in industrial automation. These factors range from frequency of operation, transmission distance, and data rates among other parameters. Protocols have to be intelligently chosen to get the maximum efficiency for a given application.

CHAPTER 3

Wireless Network Protocols

A protocol is defined as the collection of rules or conventions for data communication. It features the procedures for data representation, signaling, authentication and error detection required to send information over a communication channel [10]. When wireless was first conceived for use in industrial automation it was easier to use the existing information technology protocols, but as applications increased the need for a standard industrial wireless protocol grew. The use of one or the other protocol is governed by the application it is used for and the capabilities and limitations of each protocol.

There are different protocols available for industrial automation and major standards are described here: IEEE 802.11-based Wi-Fi, IEEE 802.15.1-based Bluetooth, IEEE 802.15.4-based ZigBee, WirelessHART and ISA SP100.11a.

3.1 IEEE 802.11

The IEEE 802.11 is one of the earliest standards to be approved for wireless network in July 1997, which was straightforward extension of the wired Local Area Network (LAN) [13]. For path sharing the 802.11 specifications uses the Ethernet protocol and Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Given the flexibility to be implemented in either infrastructure mode or ad-hoc mode, it

had allowed for smooth transition from wired network to wireless without major system changes and constraints [14].

The IEEE 802.11 standards work on the ISM bands 2.4 GHz (b, g, n) and 5 GHz (a, n) and transmission power is approximately 100 mW for 100 meter range. It uses access points to connect to the end devices and each of these access points can connect to a maximum of 255 client devices, with 128 devices operating simultaneously. 802.11 use IEEE standard Wired Equivalent Privacy (WEP) to provide data security, authentication and data encryption. Authentication is offered using a shared or an open key whereas data is encrypted using WEP 64-bits or 128-bits for 2.4 GHz systems and 152-bits for 5 GHz systems [14].

The most popular and widely used versions of IEEE 802.11 in industries are tabulated in the below table [9].

Standard Designation	Operational Frequency	Transmission Method	Maximum Data Rate	Maximum Distance
IEEE 802.11b	2.4 GHz	DSSS	11 Mbps	300 feet (100 m)
IEEE 802.11a	5 GHz	OFDM	54 Mbps	300 feet (100 m)
IEEE 802.11g	2.4 GHz	OFDM, DSSS	54 Mbps	300 feet (100 m)
IEEE 802.11n	2.4- and 5 GHz	OFDM	54 to 600 Mbps	820 feet (250 m)

Table 3.1: Wi-Fi Characteristics

3.1.1 IEEE 802.11b

The IEEE 802.11b was the first standard of this family to be used in WLAN applications, and is based on Direct Sequence Spread Spectrum where the data is spread

over a frequency range using a spreading algorithm. It uses the ISM 2.4 GHz spectrum which can work well in an indoor environment where there are physical obstacles as walls and roofs. It can offer a data rate up to 11 Mbps serving a diameter of around 100 meters or 300 feet. The data rate drops as the distance between the transmitter and receiver increases, dropping to as low as 1 Mbps. It has found application in homes and business where users can access internet, share files and applications [14].

3.1.2 IEEE 802.11a

The IEEE 802.11a device communicates at a higher data rate of 54 Mbps in 5 GHz band and was developed as a high speed alternative for 802.11b. It uses the Orthogonal Frequency Division Multiplexing (OFDM) transmission method in which sub-signals are transmitted over different frequencies simultaneously. This reduces the amount of interference and the signal-to-noise ratio [13]. It has a range as much as 802.11b in the vicinity of 100 meters. The major between the 802.11b, and –a, is that 802.11a provides higher speeds and wider bandwidth at the cost of shorter range and higher power consumption. Another point to be noted is 802.11a and 802.11b are not compatible and as a result did not find much usage in the market for long [13]. As an alternative, IEEE 802.11g was developed.

3.1.3 IEEE 802.11g

The IEEE 802.11g was developed to provide higher speed transmission at the range of 54 Mbps as the 802.11a but it also offers backward compatibility with 802.11b.

The compatibility is achieved by using the DSSS transmission method of 802.11b for speed of 11 Mbps and uses more efficient OFDM for higher speeds up to 54 Mbps [13].

Since it uses the same 2.4 GHz and not 5 GHz, the problems of smaller bandwidth persisted that offered lower capacity.

3.1.4 IEEE 802.11n

The recently standardized (in 2009) IEEE 802.11n [15] offers the best of all the worlds in the 802.11x series. It offers backward compatibility with all of its predecessors discussed here with five times throughput and twice the reliability and predictability. It has multiple antennas and multiple input and multiple output (MIMO) capabilities that increase the throughput considerably and maintaining the fidelity of the data transmitted. It offers high speed performance in comparison to its wired counterparts to a maximum of 600 Mbps. Its operating range is considerably higher serving an area of 250m in diameter, and up to 300,000 packets/sec of data transfer is possible using multiple radios and channels.

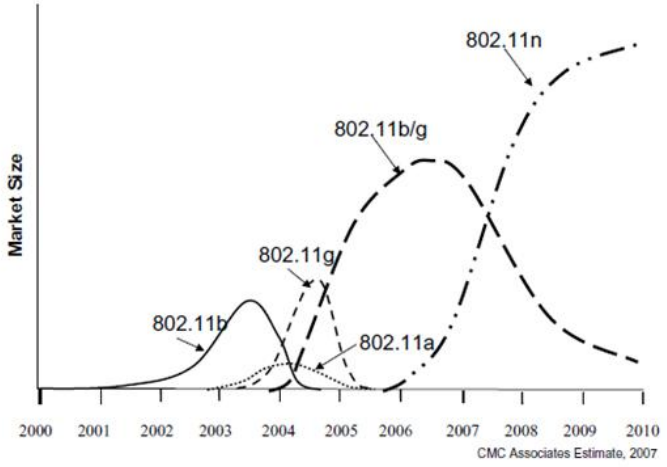

Figure 3.7: Roadmap for IEEE 802.11 standards

3.2 IEEE 802.15.1

The Bluetooth concept was conceived in 1994 when Ericsson Mobile Communications began a study to examine alternatives for voice and data cabling. Bluetooth Special Interest Group (SIG) was founded in 1996 with 5 members and others were invited to join Bluetooth Adopters and now the SIG now has over 2000 members from various fields [17].

Bluetooth, mainly used for data and voice wireless transmission, is more of a communication application stack whose lower two communications PHY and MAC have been published in the IEEE 802.15.1 standard. Bluetooth wireless technology is a robust secure short-range wireless communication protocol developed as a cable replacement for computers and hand-held devices. It is an omnidirectional and just like IEEE 802.11 uses unlicensed ISM 2.4 GHz frequency band. The band is split into seventy nine channels in most part of the world that operate between 2.4000 GHz and 2.4835 GHz. It can communicate through physical obstacles, ranging from 1 meter to 100 meters depending on the class of use. Class 3 transmits 1 mW and covers 1 meter, whereas Class 2's power is 2.5 mW for a range of 10 meters and Class 3 has a maximum range of 100 meters for a transmission power of 100 mW. It uses the frequency hopping spread spectrum at the rate of 1600 hops/second for the connection type [16].

Bluetooth offers forward error correction technique for better delivery of data but this eats up on the transmission rate. The earlier versions of Bluetooth provided data rate up to 1 Mbps which significantly increased to date up to 24 Mbps.

The data is Gaussian Frequency Shift Keying (GFSK) modulated and the security is provided at multiple levels. Bluetooth specifies security at the link level and each of the

application specifies its Application-level security. It uses a 128-bit key for data authentication and the key size is configurable between 8 and 128 bits for data encryption [14].

Bluetooth has a unique topological organization that uses master-slave relationship between nodes. Each node can communicate only to a maximum of eight nodes, and this network makes a piconet. In each piconet, there is assigned one master whose clock and hopping sequence is used to synchronize all other slaves within the piconet. A slave in a piconet can be a master in another piconet, expanding the network to more than one level. Since the nodes can accommodate point-to-point and point-to-multipoint communication, several piconets can be established and together can form a larger network of many levels called scatternet [14].

As discussed earlier the PHY and MAC layer of Bluetooth is based on IEEE 802.15.1, the Bluetooth SIG has defined 13 profiles for various applications. Table below details the various Application profiles [9]:

Profile	Description
Generic Access	Describes how two Bluetooth stations begin communicating
Service Discovery	A standardized procedure to locate and identify Bluetooth services
Cordless Telephony	Services for cordless telephones
Intercom	Services for intercom and paging or walkie-talkie usage
Serial Port	Services to emulate a serial port connection
Headset	Services to support headphones and a microphone for full duplex voice communications
Dial-Up Networking	Services to allow a computer to use a cellular phone or modem as a wireless modem for connecting to a dial-up Internet access server or for using other dial-up services, including receiving data calls
Fax	Services to allow devices to send or receive fax messages
LAN Access	Services to allow devices to become network nodes on a LAN
Generic Object Exchange	Services for transporting data
Object Push	Services for sending, pulling, and exchanging data
File Transfer	Services for browsing and transferring files
Synchronization	Services to support file update processes between devices

Table 3.2: Bluetooth Application Profiles

3.3 IEEE 802.15.4

The IEEE 802.15.4-2006 standard designates the physical and the data link layer or the media access control layer of the OSI 7-layer model for ultra low-power and low data rate wireless Personal Area Networks (PANs). Many communications protocols where applications demand low power and doesn't require high speed use this standard in their PHY and MAC layer. Also the simplicity of this standard also dictates their use in development of industrial communication protocols such as ZigBee, WirelessHART, and ISA SP100.11a.

The significant goals of 802.15.4 are low power leading to a low complexity and simple protocol. To maintain simplicity of the standard, data rates are defined between 250 Kbps and 20 Kbps for communication [18]. Low power consumption is achieved by allowing the nodes to sleep during non-operational time and each node in a typical setup is planned to sleep for 97.5% of the time promising low duty cycle [9].

The PHY and MAC layers for IEEE 802.15.4 standard is illustrated in the below figure.

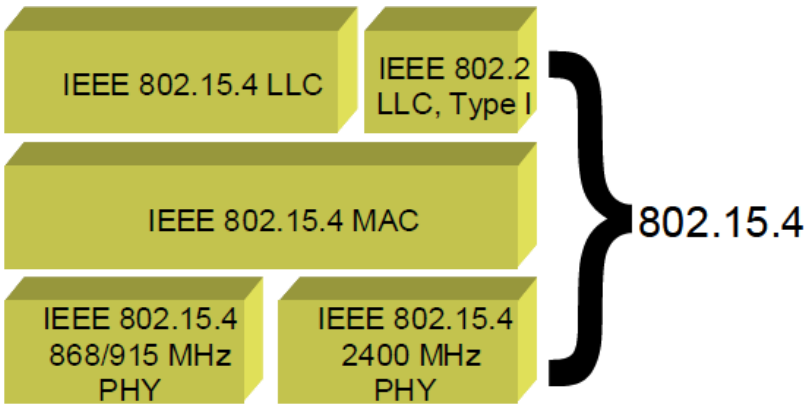

Figure 3.2: IEEE 802.15.4 PHY and MAC layers

At the physical layer, the radio can operate at three different frequency bands, 2.4 GHz, 915 MHz and 868 MHz ISM bands [19]. The number of channels in each of these bands various geographically but the sixteen channels in the 2.4 GHz ISM band can be used universally. The transmission method defined by the standard for modulation uses direct sequence spread spectrum (DSSS), which spreads the signal over a range of frequencies using a spreading algorithm. This way the electromagnetic interference and the noise can be reduced for a distance up to 100 meters.

The data link layer offers network beaconing, associates nodes, validates frame apart from assuring time slots for communication [18]. Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) is used for more reliability. Either non-beacon or beacon modes [9] can be used for transmission depending on the complexity of the network. Non-beacon mode is used for simple networks and beacon mode is used for complex networks. In beacon mode, collisions are avoided by assigning nodes to transmit to one of sixteen time slots by the network coordinator. The advantage of using beacon mode helps saving power in the battery operated devices by putting the devices to sleep when they are not transmitting or receiving. They come back to life in their time slot, takes the action and goes to sleep again. By this method, a node is expected to sleep or be in the idle state for about 97.5% of the total time.

Networks can be built using only two topologies by IEEE 802.15.4 at the data link layer [19] – star and peer-to-peer or point-to-point. But the peer-to-peer topology can be extended to form a meshed network or a clustered tree network to maximize the range of operation. Also, each device in the network has a unique 64-bit identifier or 16-bit identifier can also be used in smaller applications.

3.3.1 ZigBee

ZigBee is a low-cost low-power networking standard based on IEEE 802.15.4 developed by the ZigBee Alliance primarily for monitoring and control products. It is a high level communication protocol suite that differentiates itself from WPANs such as Bluetooth by being simple, providing long battery life but still accomplishing security in the network.

ZigBee's strengths include low-cost – wide applications, low power – long battery lives and it supports mesh networking thereby increasing both reliability and coverage area. Although wireless meshing topology increases complexity of the network and the latency, it can be overcome by rightly planning the network deployment according to the application.

Many manufacturers are providing cheaper system on a chip (SoC) solutions that has a microprocessor integrated with an antenna for easy development. The ZigBee protocol stacks along with the IEEE 802.15.4 PHY and MAC stacks can be easily deployed on the microprocessor to obtain a cost effective wireless solutions. ZigBee has found usage in wide applications and industries particularly in home, building and industrial automation.

ZigBee operates in the 2.4 GHz frequency band worldwide but also have the option of 915 MHz and 868 MHz in different regions. Longer battery life is possible because of the ability to activate ZigBee in no time. It takes less than 15 milliseconds [19] for the device to switch between sleep mode to operation mode which can be accommodated in a plant or factory floor.

With the possibility of mesh networking [19], devices can be classified as either ZigBee coordinator (ZC), router (ZR) or end device (ZED). There can be only one coordinator in a network setup because it has the security keys for the devices it is communicating with. ZRs are intermediate nodes that sends it own data as well as pass on the data from other nodes. And at the low level, there are ZEDs that can only transmit data to either ZC or ZR and doesn't communicate with other devices. Security in ZigBee is based on Advanced Encryption Standard, AES-128 and as such security is provided at the MAC, Network, and Application layers.

3.3.2 WirelessHART

WirelessHART was developed by HART Communication Foundation based on the proven and familiar Highway Addressable Remote Transducer (HART) Communication protocol and was released on September 07, 2007. This protocol is therefore, two years in market now and recognized as international standard by International Electrotechnical Commission (IEC) as IEC 62591 Ed. 1.0 from April 6, 2010. Wireless HART is based on IEEE 802.15.4 that provides the low-cost and low-power advantage.

WirelessHART was developed to improve the capabilities of existing 30 million HART devices installed in the plant that doesn't tap the full functionality of HART protocol. HART protocol was developed 30 years back that revolutionized the data communication technique between the field devices and the controllers. It uses 4-20 mA analog current range to transit the process variable and digital information about the process and the instrument is sent along with the analog information.

In most scenarios, HART devices are only used to transmit the process variable via the cable and bulk of the useful information is untapped which can help in the instrument and plant optimization. In 2006, HCF started developing a standard and the result of this process is WirelessHART - wireless mesh network communications protocol that adds wireless capabilities to the HART Protocol while maintaining compatibility with existing HART devices, commands, and tools.

Apart from being open and interoperable standard, it fulfills the real-time constrains imposed at the field level in a typical control system. It has proved to be robust, reliable and secure for monitoring and is industry is taking calculated steps to implement the standard for closed-loop control.

WirelessHART can be implemented with the existing HART devices and increase the capability but also new devices are developed as an upgrade to HART devices that could provide analog information through the wired control system and the digital information wirelessly to asset management systems and maintenance systems. In a typical WirelessHART implemented network, there are nodes that transmit the data to a gateway wirelessly, which is further connected to the host control system through any of the existing wired protocols such as Ethernet.

As with the case of ZigBee, WirelessHART also uses IEEE 802.15.4-2006 standard for Physical and Data Link Layer. It uses the universal 2.4 GHz frequency band divided into 16 channels with feature of low duty cycles to maximize battery life. Mesh routing technique is used to increase reliability and extend the operating distance. All nodes in WirelessHART can act as trans-receivable routers providing full ability for mesh

topology. Interference and predictability is increased through the channel hopping between 16 channels using fixed frequency hopping transmission method. Additionally, WirelessHART uses Time Division Multiple Access (TDMA) to optimally maximize the time slot for longer messages.

There always exists multiple paths from the end nodes to the gateway for reliability and the network automatically optimizes the route choosing the best route always in order to minimize latency. Routing [9] is the responsibility of the upper Data Link Layer and the Network layer between the nodes, and nodes and gateway using the graph routing technology.

The Transport layer [20] provides a combination of both un-acknowledged and acknowledged transmissions and in case of failed delivery it attempts to transmit again. Segmentation of data from the application is done at this layer for transferring data such as waveform has a large data size. Unicast, multicast and broadcast transmissions are all supported at this layer.

There is no defined Application layer, but data may be polled from the node by request or using some kind of alerting function that transmits when the process variable shoots over set limit. AES-128 encryption technique is used for data encryption in WirelessHART [9]. As with beacon implementation in ZigBee, each node wakes up every 10 milliseconds [20] for either for passing the data or giving its own data to optimize battery life.

3.3.3 ISA SP100.11a

ISA SP100.11a was developed by International Society of Automation (ISA) as part of ISA SP100 standards for wireless communication in industrial environment and was released on September 09, 2009. This protocol is therefore, is in market for only a year now and yet to be recognized by International Electrotechnical Commission (IEC) and ANSI as an international standard.

The standard was developed as a low-power, low-cost, low-data rate to provide robust, reliable and secure wireless operation for non-critical monitoring, alerting, supervisory control, open loop control, and closed loop control applications. It also boasts of providing reliable data communications in harsh industrial conditions and can tolerate latencies up to 100 milliseconds. It has strategized its plan to operate in wireless crowded environments by cooperative operation in order to minimize interferences.

ISA SP100.11a is based on IEEE 802.15.4 – 2006 (PHY and DLL) and includes a 2.4 GHz radio. As with WirelessHART, this standard also uses Time Division Multiple Access (TDMA), DSSS and Channel hopping to support interoperability, eliminate interference, reduce noise and increase channel reliability. Mesh routing capability increases the coverage area in the network for scalability but at the cost of latency.

The network layer [9] of this communication protocol stack provides addressing, inter-networking routing and routing outside the network. It uses the Internet Protocol Ver. 6 (IPv6) frame formatting providing the standard 128-bit IP names to the nodes, but generally to avoid intrusions in to the ISA network, 16-bit short addressing is used to address the local nodes.

The Transport layer [9] supports all of the broadcast, unicast and multicast techniques of data transfer. It also provides transparent transfer of data between the hosts. The end-to-end recovery is also possible through the transport layer using the services such as acknowledged and unacknowledged transfer and flow control.

The application layer in the ISA SP100 should work with the existing systems or protocols available in the industry such as the Fieldbus, HART, Profibus, DeviceNet, and others. This demands tunneling protocol capability that would allow the network to work flawlessly with the existing protocols. To maximize the battery life of the devices native protocol capability is interwoven that makes use of efficient bandwidth usage.

Security is a major consideration of any protocol stack and many layers of OSI models offers security, MAC layer blocks outside-of-network infringement and network layer safeguards the network with-in the network. For data encryption and authentication the standard uses AES-128 or 256 encryption keys or public / private encryption keys [9].

To minimize power consumption, nodes uses the beacon technique in which the devices sleep most of the time and is called upon only when a data a required of it or it routes a data packet. As against WirelessHART, not nodes can act as routers and they are configurable to be used as end devices, routers or coordinators. A gateway is used to communicate between the ISA SP100.11a devices with the host control system, with the protocol translation abilities provided at the application later.

3.4 SUMMARY

To tailor the right protocol to its intended application it is important to understand the fundamental differences of the industrial standard protocols. This chapter detailed the

technical specifications such as the data rate, frequency, transmission distance, channel hopping techniques, security features, powering issues among others of the protocols, which have the potential to be implemented in the plant and factory floors.

The protocols were broadly classified in to three categories IEEE 802.11, IEEE 802.15.1 and IEEE 802.15.4 based standards and studied in great depth.

CHAPTER 4

Comparison of Wireless Protocols

After the studying the advantages of wireless technology over their over counter parts and the different wireless technologies available this chapter would detail the comparison of the various protocols available or use in the industrial monitoring and control. Before we could dive in to this topic, it is important to understand the requirements of data communications in industrial environment which is largely different than that of home and business deployments of wireless.

The automation in industries can be implemented for factory or a process plant, and the difference between them is factory employ discrete manufacturing techniques while in the plant the product continuous flows such as liquid or gas. Environment varies widely in these two applications and understanding it would be useful for wireless deployment. Factories as mentioned uses metal cutting, welding and fabrication of unit parts or products in an assembly lines or product lines. There are often noisy, dusty, and oily and the temperature is usually in the ranges where humans can work. A plant, on the other hand, usually processes chemically a hydrocarbon raw material and produces a hydrocarbon output. The temperature and pressure in such processes can reach up to thousands of Kelvin and Pascal and usually the areas of operation are corrosive, poisonous and flammable. The plant is setup in open environment mainly, which can experience all the seasons of the year.

Safety is a primary concern in both of these industries that involves hundreds of man power and millions of dollars in equipments and these cannot be compromised at any cost. The design of the control system should not only optimize the production of the plant but also take into considerations of safety of the personnel and equipments. So the data communicated by the field devices should reliably come to the control room and the appropriate control action should be relayed back to the field. The channel of communication should be free from error, frame loss and data losses. Also, the data transmitted should be secure so that there are no foreign intrusion in to the network, as this could compromise the safety of the plant or factory. Intrusions may cause havoc by upsetting the control system or by acquiring data that could be of economical values.

Finally, the power requirements should be considered at the installation of measurement nodes. Remote applications may pose a constraint on the power availability and in these cases running a power cable would not be feasible. Also, mobility will be impaired when the device is connected to a power socket. Also, the power consumptions of devices also varies, a pressure or transmitter requires lesser power than a flow meter or vibration meters. In conclusion, to operate a device wirelessly it is important to consider external factors such as environment of use, security, data type, power requirement, etc. and understanding them would help us choose the best technology.

4.1 SPECIFICATIONS-BASED COMPARISON

In the previous chapter, different protocols available for industrial automation were analyzed and detailed technically. This section would compare the fundamental engineering principles behind these protocols and the point the differences in them and

how it would affect its deployment in the field. Data rate, frequency of operation, transmission distance, bandwidth, data throughput, signal-to-noise ratio, the transmission technique used to avoid interference, noise reduction techniques, security and power consumption are few of the bases chosen for evaluation.

4.1.1 Wi-Fi

IEEE 802.11 – based Wi-Fi uses 2.4 GHz or 5 GHz radio with an operating range from 100 to 900 feet. It has a higher bandwidth for use from 11 Mbps to up to 400 Mbps and to reduce interference and noise, it uses a range of transmission technique from DSSS to OFDM [13].

It offers the security as the Ethernet and also requires the node to be on all the time requiring higher power than other protocols. Also, the feature of mobility is limited in Wi-Fi applications as signal degrades with the movement of the node. Since its data rate is also high, the nodes needs to externally power as batteries cannot be used to power them continuously for long use. It can be easily installed in places where Ethernet are in existence in the plant and provides a good alternate for this application.

4.1.2 Bluetooth

Bluetooth also has high power requirements but is considerably lower than Wi-Fi because of lesser bandwidth Bluetooth uses. It uses a 2.4 GHz radio and uses frequency hopping technique at the rate of 1600 hops per second to reduce interference. Transmission distance ranges from 1 to 100 meters, and as a result it can be employed where the coverage area is lesser for maximum throughput. Data rate for Bluetooth

ranges from 1 Mbps and it has been significantly increased up to 24 Mbps. It provides multiple layers of security, and in industrial environment Bluetooth can be used to send I/O, serial, or Ethernet data but it requires large memory requirements because of the software stack it employs.

4.1.3 ZigBee

ZigBee uses the low-power, low-data rate IEEE 802.15.4 – based PHY and MAC layers and operates in the 2.4 GHz frequency band worldwide but also have the option of 915 MHz and 868 MHz in different regions. ZigBee uses Advanced Encryption Standard, AES-128 for data encryption for security and has data rates ranging between 20 kbps to 250 kbps.

The advantage of ZigBee over the previous two protocols is its ability to operate in sleep-awake-transmit-sleep cycle, which greatly increases the battery power to up to 5 years. It enables star, cluster or mesh topology for operation which also increases the reliability and the coverage distance to more than 300 feet but at the cost of increase in latency. ZigBee uses the DSSS transmission technique offered by the parent standard to reduce the interference and noise reduction.

4.1.4 WirelessHART vs. ISA SP100.11a

As these protocols were developed for the sole purpose for factory and plant automation, it is only sensible to compare these protocols head to head. The difference between the two protocols draws an analogy of Windows PC and Apple MAC. WirelessHART uses the existing HART communication protocol, thereby allowing easy

integration of wireless on existing instruments with lesser wireless infrastructure. The objective of WirelessHART was to extend the de facto industry standard HART protocol, while ISA100 standard is focused on development of standard for industrial automation embracing all the wired protocols in the industry.

They both use the IEEE 802.15.4 – based PHY and MAC layers using the very similar 2.4 GHz radio, TDMA, DSSS, channel hopping and mesh routing techniques but the difference lies on the upper layers in the OSI model. ISA100.11a allows hopping between all 16 channels of the 2.4 GHz ISM band providing means to exclude any channel whereas WirelessHART uses 15 channels [9]. The usage of timeslots for communication also varies between the two protocols; WirelessHART uses a fixed 10ms time slot whereas ISA100.11a allows the use of variable time slot. Although Advanced Encryption Standard (AES) [9] is used for data encryption, WirelessHART uses only AES-128 whereas ISA100.11a has the flexibility to use either of AES-128 or AES-256, the latter providing more security with the increased key size.

The addressability of the node also differs in both WirelessHART and ISA100.11a. Although both use 16-bit short addressing for the nodes, ISA SP100.11a can use the IPv6 addressing capacity of 128-bit whereas WirelessHART uses 64-bit for unique addressing. External routing is possible as ISA100.11a uses a IETF standard Network Layer for routing messages whereas WirelessHART is impaired of such function [9].

WirelessHART can be considered as a subset of ISA100 because of the former embracing only HART technology whereas ISA's capability to embrace Fieldbus, Profibus, DeviceNet and other protocols in an existing environment. At this point of time,

WirelessHART offers more interoperability as it was standardized two years ago, field tested and many vendors are manufacturing WirelessHART products compared to ISA100.11a which was ratified last year and yet to be approved by IEC and as a result few vendors have manufactured ISA products.

4.2 APPLICATION-BASED COMPARISON

Each application dictates its technical requirements and as a result the choice of protocol would be based on the application it would be deployed for. As mentioned in Chapter 1, there are three layers in distributed control systems that could be switched to wireless instead of the traditional cabling. At level one, wires that run from field devices to the controllers in the control room are real-time applications and transmit data at a low rate. The type of information communicated is also not in large amounts and in most cases is a digital ON/OFF or a 4-20 mA analog signal. Also, the field devices both instruments and actuators require less power as compared to power-hungry workstations in the control room, as they are less complex devices.

Typically at this level, IEEE 802.15.4 based WirelessHART, ISA 100.11a or ZigBee are intended for monitoring and control using analog and digital input/output. As they meet the requirements of less power, and also transmit data a lower rate. The choice of these protocols greatly depends on the existing resources and networks in the plant, wireless product availability and standard availability. All of three protocols can be used to build a new network of data measurement points in a plant. ZigBee offers the cheapest and the easiest solution for a small network of devices as it was built for this usage. For

up to 250 devices proven-WirelessHART can be used, and for higher scalable nodes ISA SP100.11a offers a good option.

In an established plant, that have wired HART instruments, WirelessHART adapters can be used to harness the digital data from these instruments as it offers backward compatibility with HART. Also, new WirelessHART devices can be installed to draw the advantage of de facto HART technology as well as achieving wireless connectivity. Also, WirelessHART devices are easily available from different manufacturers as the standard has been ratified two years back and they offer vendor interoperability. It has been proof tested at the plant level and an obvious choice at this point. But in plants where the existing networks uses Fieldbus, Profibus or DeviceNet, using ISA SP100.11a is only solution available to upgrade it to wireless connectivity. This protocol also offers more nodes to be supported in one network, thereby reducing the interference in a crowded environment.

Bluetooth can be used to transmit serial or Ethernet data but it consumes more power than IEEE 802.15.4 based protocols. Bluetooth can be used to replace traditional serial connections using RS-232 or RS-485 standards, and it can also be used to replace Ethernet over short distances. Power consumption and data rate using Bluetooth is between ZigBee and Wi-Fi, and it offers a mid-choice in applications with such requirements.

At the Level two of the DCS, the connection between workstations and the controllers or gateways are usually done with Ethernet which can be easily replaced with Wi-Fi. There are a number of Ethernet to Wi-Fi adapters available in the market that can implement wireless at this layer. The operating range of Wi-Fi is 100 meters and the

mobility is not offered by wireless, should applications fall within this limiting factors. Also in cases of measurement and monitoring in the field that requires that require very fast data transfer where there are easy availability of power source Wi-Fi is a viable option.

4.3 CASE STUDIES

The following cases are actual industrial situations where the need of wireless has grown and is immensely desired for its obvious advantages. It was chosen to illustrate the various problems each situation poses and the best wireless technology that could be implemented in such conditions. The cases were taken to demonstrate of application of Wi-Fi, ZigBee, WirelessHART and ISA SP100.11a. The factors used to choose the best technology were technical requirements, specifications, environment, data types, operating distance, power availability, and cost.

4.3.1 Case: Well-head Fracturing Pump

In extraction of oil or gas from a well, the fluid would flow naturally because of the pressure they are at under the earth. After, few years of extraction when 60-70% of the oil is extracted the pressure levels drop and there is no output from these wells. These wells are called “dry wells”, and are usually left unattended. Since, there has a been a scarce of oil resources and new exploration are expensive, efforts are put to pump the left over oil or gas from the dry wells to increase the efficiency of wells. Many methods are used to increase the production of wells and one such method is use of fracturing pumps. These devices are typically reciprocating devices mounted on trucks in onshore facilities

and barges in offshore that “fracture” the earth underneath to increase the permeability of the earth thus increasing the ease of flow of oil or gas through these pores created.

The fracturing pumps have a number of instruments mounted on the truck such pressure, temperature, flow instruments, tachometers, and vibration monitors. These values are fed in to a Programmable Logic Controllers in each truck that uses these values to determine the rate at which to run these pumps. For each well there are a number of pump-mounted trucks that operate paralleling in fracturing the earth and are connected through the wires to the data center (control room) to view the process variable and to stop a pump or the entire system if required.

Since these trucks are operated in harsh environments with dusts, ice, and snow most of the system shut down occur because of the faulty wires. And replacing these wires takes physical efforts and time and each shutdown causes a huge amount of money in losses. As a result, having the connectivity through wireless would reduce the down-time and connection losses.

In this case, data centers are located within 40 to 50 meters from the trucks and there is e-m noise from the mechanical working of the pumps. Since it transmits logging data from the PLC to the data and also vibration data, the data structure is also considerably bigger and higher data rate is preferred. Also, since the PLCs and pumps run through diesel generators obtaining the electricity to power the device should not be a problem.

From the description of the system it can be concluded that Wi-Fi is the most viable solution for this application as it demands higher data rates and also the operating distance is within 100 meters. Since, the power is also easily available there should be no

concern about the usage of battery in Wi-Fi. The application of Wi-Fi in fracturing pumps case would be to have an access point (AP) in the data center and have Wi-Fi nodes in each of the trucks that transmit the information. The PLC in the truck can be connected to the Wi-Fi adapter serially, and with the right configuration of the PLC and AP data acquisition system, connectivity with the advantageous wireless is possible. This is one such real-time application of wireless in a harsh and crowded environment where connecting through wireless can decrease the downtime considerably and also save on the cabling costs.

4.3.2 Case: Oil and Gas Pipelines

Oil and gas are produced at remote well sites both onshore and offshore and this level is a black fluid or gas combined with water which has no usage in the real world. This needs to be processed to more usable hydrocarbons at the refineries or processing units. Normally, production of oil or gas happens at upstream and the refining is done downstream which may be miles apart and needs to be transported through pipelines. Also, the processed oil or gas is also transported to different parts of the country through pipelines. These pipelines run through remote part of the country away from human interruption for security reasons.

The terrain usually varies and can run through arid deserts, snows, and other bodies, but it is really important that these pipelines remain in good shape to save the environment and also for safety of the inhabitants nearby as the transported material can be poisonous and flammable. It is really important to check the health of the pipelines regularly and running cables for thousands of miles to monitor the situation is impossible

both physically and monetarily. Also, physical human inspection is also not possible and even done requires a huge number of work force to keep this pipeline safe.

The solution in such a case is to have wireless option which can relay the health of the pipeline to the main control room. Since, there is no power available in most of these areas, the information it transfers is not more than few bytes, and there is no need of continuous monitoring one of the IEEE 802.15.4 based protocols could be deployed in this application - ZigBee would be the least complex, least cost in this application as it is turnkey or built from scratch.

There can be wireless ZigBee devices installed that measure the pressure and flow at each of the segmented areas of a long pipeline and transmit this data a gateway that could be connected to the control room using GSM/GPRS. Since, ZigBee uses relatively low power and there is no need for continuous monitoring they could be powered by batter pack and usually they run for about five years. The gateway receives the data from ZigBee modules and translates the data to be sent using satellite communication and can be battery-powered as well. It can use a simple star topology between the devices and the gateway. With this installation, the health of the pipelines could be monitored cost efficiently and if there are any alerts raised by this measurement system suitable action can be taken to prevent environmental disasters apart from saving lives and money.

4.3.3 Case: Upgrading an Existing Well-head offshore Platform

Offshore platforms are structures that are built in the seas to produce oil and gas from the wells below the ocean bed. When offshore platforms are built the type of control

system employed would be DCS and often they wouldn't be scalable after a certain number of I/Os are reached. It is also because of wiring complexity and limits in termination of the marshalling and junction boxes it becomes difficult to add a new instrument in an offshore platform to the DCS.

Also, in the DCS the usage of HART devices are considerably higher of and almost 85% of installed devices are HART enabled. The DCS always dynamically grows in a platform because of the addition of few measurement points, or addition of a well head, or it is important to tap the digital information from the existing HART devices.

In such cases, the use of WirelessHART as a means to obtain connectivity is an obvious solutions since it does not require any cables to be run from the control room and also because of the backward compatibility it offers with the HART devices. A WirelessHART adapter can be attached to a wired device and the adapter can wirelessly transmit the process variable and the HART data to the gateway that connects to the existing host control system or asset management system. A free standing WirelessHART device can be installed that can transmit the process variable and HART data wirelessly to the gateway.

WirelessHART offers low-cost, low-power option that maximizes the battery life of the devices which offers secure, reliable and robust connections in the upgrade of the platform and not interfering with the existing networks and the infrastructure. It also provides a safe closed-loop control application as it can be seen from the below figure in where the process is trying to control the pH content of a solution using WirelessHART.

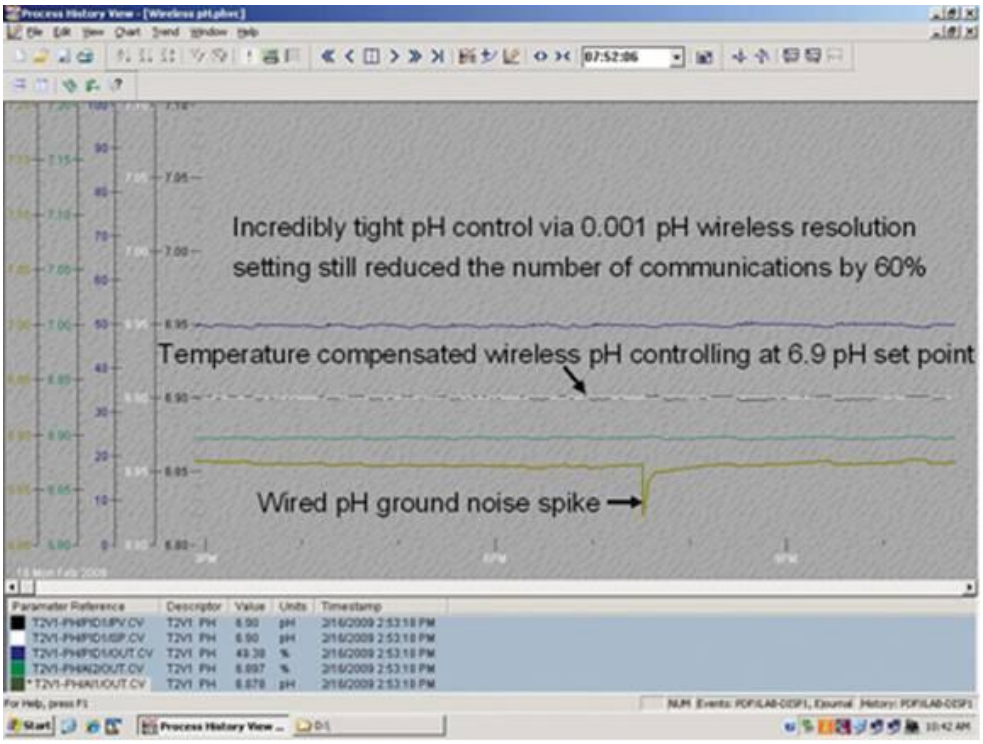

Figure 4.8: Closed-Loop Control using WirelessHART (Source: HART Communication Foundation)

4.3.4 Case: Turnkey Refinery Expansion

Refineries and other hydrocarbon processing facility exhausts the gas trapped in the flanges, relief valves and other devices to the atmosphere causing environmental pollution. These gases are called flare gas, because just before they are let out in the atmosphere are they are burnt to reduce the gas to carbon dioxide. As this causes air pollution and wastes a considerable amount of the useful gas, recovery units for these gas are added to the existing refineries or plants to trap these gases and bring them in to the process.

As these are new units to be added to the existing plant and have a separate control system with few interfaces with the existing DCS, wireless options are preferred

over the wired options because of the less number of the input / output points, and to reduce the cable laying overhead in an already crowded plant.

The data points for these recovery units do not scale more than thirty nodes and as such the use of mesh routing capable network with high degree of security is preferred. Low-power consumption is the norm as maximizing battery life is an important factor and also the data transferred are in the range of few hundred of bytes.

Using the IEEE 802.15.4-based ISA SP 100.11a is a viable option as it offers the reliability and security demanded by this application. Since, it is a new plant that could communicate with Fieldbus or Profibus devices, WirelessHART may not be the right option. Thirty of the ISA SP100.11a nodes can be mesh networked using a single gateway that can be connected to the host control system. The value from the existing Fieldbus devices can also be extracted to the gateway. The nodes can be mesh networked to expand to the whole recovery system and the future additions can be met with little mechanical effort.

4.4 GUIDELINES FOR CONVERTING WIRED TO WIRELESS

Having studied the advantages of wireless in plant or factory automation the next obvious question that pops is the factors that dictate the deployment of wireless in industrial automation. But before we deal that topic, it is very important to answer the question: Is wireless necessary in the existing set-up? There is no point in deploying wireless where there is no need for it for obvious economic reasons and unnecessary complications of the existing network environment.

Wireless can be implemented cost-effectively on a secondary network that may or may not integrate with the existing control system to improve the production, troubleshoot the different field instruments, help in maintenance and proactively take steps to reduce the stop times of an instrument or valve thereby cutting down the plant down-time. This can be achieved by adding wireless adapters to the field instruments to tap the secondary variables or install measurement nodes at the points of interest and communicate to the asset management systems to optimize plant operations.

Sometimes, applications demand the use of wireless instruments where installing the wired instrument is impossible or having a wired set-up is not feasible economically. For example, in cement plant the process variables in a rotating kiln is hard to measure using a wired instrument because of the rotary movement which could lead to tangling of wires. Also, in harsh, flammable, ultra-clean or bio-hazard applications use of cables or wires could contaminate the environment or melt in high temperatures, and, in such cases wired instruments cannot be installed. For remote measurement, where, wires could run for miles and where there is unavailability of power, having a wireless deployment is more reasonable than a wired approach. Also, when there is a necessity of mobility or having temporary measurement point in a system wireless is a viable option.

In all other cases where there is both wired and wireless options available in deployment for measurement, wireless would be preferred in cases where running a cable from the control system to the instrument required a lot of changes in the existing set-up. There is also the possibility of cable conduits or trays, termination boxes and junction boxes reaching a maximum capacity or less in numbers which could be used for more critical control applications. But before we dive into installing wireless, there should be a

study of the existing wired and wireless network infrastructure for easy integration and eliminating interference, mechanical and electrical equipment set-ups or obstruction study to compute the line-of-sight, choosing the best fitting standard and topology keeping in mind the future scalability of the plant. It is not wise to cluster the plant with different wireless technologies for different applications as this could hamper the plant production in the long run. Also the latency tolerated by the process dictates the number of hops or nodes between the end device and the gateway. This would outline the network set-up and the number of end devices, routers and gateways in the network. One other important factor to take into consideration is the powering options available to power the wireless nodes. As all nodes need to be powered for their operation, there are two possible powering options available: having a power cable run to the wireless instrument (only the process data is communicated wirelessly) or batteries where there is no possibility of power sockets near its applications. Since battery has a limit on the time of operation, although it may offer up to five years, it is wise to just replace the data cable many a times and have a power cable in case of its availability near the instrument.

For closed-loop control applications, wireless being a nascent technology has not gained trust to operate in critical applications as any communication failure may result in loss of lives, damage to the equipments and the environment. As a result, wireless is slowly being test-deployed in feedback control applications. One method is having cables for the instruments and actuators that are actually in the loop that alerts the controller in the cause-and-effect diagrams for control actions, and the reminder of the instruments can be connected wirelessly. This method will have the coexistence both the wired and wireless networks and the more critical control applications are wired and monitoring

requirements is fulfilled by wireless technology. Also, in this method wireless feature could be added to the field devices and actuators as a backbone control network, thus if the one of the network fails, there is always the other option available. The advantage with this is the ability to employ wireless slowly but steadily for controlling.

The other approach is a drastic and a more bold approach where the control loop devices – instruments and actuators are connected wirelessly to the host control system. To make the system fail-safe, triple modular redundant technology is used, where network can be set-up for the nodes to communicate with the gateway through three different paths completely independent of each other. There will be increase in the infrastructure with the addition of routers but will be more reliable than the single path communication where there could be moving obstructions.

As discussed, it is a huge task to embrace the upcoming wireless technology in the process and factory floors and should be deployed intelligently to extract the best results of wireless – benefitting from the advantages and avoiding the traps of wireless.

4.5 SUMMARY

This chapter drew comparison of the different standards available for industrial automation on two categories: Specifications-based and Applications-based. In specifications-based comparison, the protocols were compared on various technical specs such as: frequency of transmission, data rate, data types supported, range of operation, data encryption types, and powering issues. In the later, comparison was drawn on the different applications it could be employed and the factors were cost, interoperability and backward compatibility with already existing protocols, and level of control system at

which the wireless connectivity is employed. Also, this chapter illustrated four worldly cases of wireless implementations that is desired and produced guidelines of choosing the right protocol for their application.

CHAPTER 5

Conclusions and Future Work

A Distributed Control Systems is a widely applied form of control engineering technology where a controller or computer is distributed to each process separately and each of these local controllers is connected to a centralized controller which is further connected to the enterprise management systems. There are three layers of DCS: field, control room, and the enterprise. Traditionally, these connections between the layers and within the layer (field devices to local controller) are wired which offered the reliability and predictability demanded by the criticality of the process and discrete manufacturing industries. But with the advancements in the wireless technology in the last two decades have the automation industry turn towards it as a means of data communication media because of the various advantages it offers. Advantages include cost benefits – wireless reduces the infrastructural cost by 90% of the wired option, capability of remote operations, ability to operate in harsh and ultra clean areas, mobility, and easy scalability of the plant.

There are many characteristics of the wireless technologies to be considered when applied in the plant and factory floors and one of the most important characteristic of wireless communication is the protocol that defines the procedures and rules for data communication and choosing the right protocol for the industrial network issues is an important question to answer for wireless deployment.

The different protocols available are: IEEE 802.11-based Wi-Fi – High rate data transfer, higher power, IEEE 802.15.1-based Bluetooth – Low power, short range, medium data rates, and IEEE 802.15.4-based ZigBee, WirelessHART, and ISA SP100.11a – Ultra low power, larger scale networks, low data rates. The table [8] below summarizes the specifications of different protocols and the applications in can be implemented in industrial monitoring and control.

	Enterprise Ethernet	SCADA Ethernet	Serial Data	Analog and Digital I/O
WirelessHART, ISA SP100.11a, ZigBee Frequency: 2.4 GHz Speed: 20 to 250 kbps Range: < 100 feet				
Bluetooth Frequency: 2.4 GHz Speed: 1 to 24 Mbps Range: < 300 feet				
WiFi Frequency: 2.4 GHz / 5 GHz Speed: 10 to 420 Mbps Range: < 1000 feet				
Proprietary Frequency: 900 MHz / 2.4 GHz Speed: 350 kbps Range: 20miles				

Table 5.1: Industrial Wireless Usage

After studying the technical details and aspects of each of these protocols, it is easier to draw a comparison between them on two lines: specifications-based and application-based. In the former, the protocols were compared on various technical specs

such as: frequency of transmission, data rate and throughput, range of operation, data encryption types, and powering issues. In the later, comparison was drawn on the different applications it could be employed and the factors were cost, interoperability and backward compatibility with already existing protocols, and level of control system at which the wireless connectivity is employed. Also, four real-world cases where the use of wireless is desired because of the inability to run cables in the application were studied and based on the requirements and conditions posed by each of the cases guidelines of choosing the right protocol for their application were illustrated.

WirelessHART and ISA SP100.11a the two protocols developed for the sole purpose of industrial automation were put head-to-head technically, although ISA SP100.11a had few advantages in the specifications aspects than WirelessHART, the later because of its simplicity, backward compatibility with the proven HART technology, tested application in the fields, and more vendors manufacturing these units have given WirelessHART an advantage. ISA SP100.11a is developed to encompass technologies other than HART such as Fieldbus, Profibus and DeviceNet but it is still natal stages of applications in the field. WirelessHART is also recognized as IEC standard which also gives a competitive advantage for its application over ISA SP100.11a (as of November 2010).

But, both the standards' organizations are working together for to find a point of convergence where both the protocols can be merged in to one or at least have the option of interoperability between these protocols. It is still in the initial stages of discussion and there is no convergence in sight as of end of 2010.

In the future, the research in this field can be extended in to study of other protocols such as WiMAX (Worldwide Interoperability of Microwave Access), cellular technologies such as 3G or the new 4G, Ultra Wide Band (UWB) – WiMedia and Direct Sequence-UWB which are upcoming technology some of this offers faster data rates at low power. Further the use of wireless in industrial applications can be widened, by moving to a state where are just one or two wireless standards to reduce complexity and as long as there is enough distinction between the standards. So the focus should be on the convergence of the standards to reap the true benefits of wireless in industrial automation.

References

[1] Krishna Kant, *Computer-based Industrial Control*, 4th ed., Prentice Hall of India, 2004.

[2] Mark Nixon, Rusty Shepard, Aloysius K. Mok, Bill Bennett, and Deji Chen, "Process Control Adopts Wireless", *InTech ISA*, Feb. 2005.

[3] J. Colandairaj, G. Irwin, and W. Scanlon, "Understanding Wireless Networked Control Systems through Simulation", *IEEE Computing & Control Engineering*, vol. 16, no. 2, pp. 26-31, Apr. 2005.

[4] John S. Seybold, *Introduction to RF propagation*, Wiley, 2005.

[5] Theodore S. Rappaport, *Wireless Communications – Principles and Practice*, 2nd ed., Prentice Hall of India, 2007.

[6] Jochen Schiller, *Mobile Communications*, 2nd ed., Pearson, 2007.

[7] Simon R. Saunders, Alejandro Aragon-Zavala, *Antennas and Propagation for Wireless Communication systems*, 2nd ed., Wiley, 2007.

[8] Ira Sharp, "Wireless in Control Systems", *Automation.com Journal*, Oct. 2010.

[9] Dick Caro, *Wireless Networks for Industrial Automation*, 3rd ed., ISA Publication, 2008.

[10] John Park, Steve Mackay, and Edwin Wright, *Practical Data Communications for* Instrumentation and Control Systems, Elsevier, 2003.

[11] Peter Welander, "Topologies for Wireless Instrumentation", *Control Engineering*, pp. 48-56, Nov. 2007.

[12] Peter Welander, 3 approaches to Process Plant Wireless, *Supplement to Control Engineering*, pp. 3-7, Aug. 2007.

[13] Martyn Mallick, *Mobile and Wireless Design Essentials*, Wiley, 2003.

[14] Nathan J. Muller, *Wireless A to Z*, McGraw Hill, 2003.

[15] David Tung Chang Wong, Peng-Yong Kong, Ying-Chang Liang, Kee Chaing Chua, and Jon W. Mark, *Wireless Broadband Networks,* Wiley, 2009.

[16] Jennifer Bray, and Charles Sturman, *Bluetooth: Connect Without Cables*, Prentice Hall, 2001.

[17] MMS Anand, *Electronic Instruments and Instrumentation Technology*, Prentice Hall India, 2004.

[18] Houda Labiod, Hossam Afifi, and Costantino De Santis, *Wi-Fi, Bluetooth, ZigBee and WiMAX*, Springer, 2007.

[19] Drew Gislason, *ZigBee Wireless Networking*, Newnes, 2008.

[20] Deji Chen, Mark Nixon, and Aloysius Mok, *WirelessHART: Real-Time Mesh Network for Industrial Automation*, Springer, 2010.

Vita

Mohamed Shahid Abdul Ghayum was born in Chennai, India and was brought up in the city of Dubai, United Arab Emirates. He completed his Bachelor's (Honors) in Electronics and Instrumentation Engineering from Birla Institute of Technology and Science, Pilani, – Dubai Campus, United Arab Emirates. Mohamed decided to specialize in the area of automation and began his graduate studies at the Department of Electrical and Computer Engineering at The University of Texas at Austin in August 2008. For his Masters research, he worked under the supervision of Dr. Aloysius K. Mok of the Department of Computer Science.

Email: mohamed.shahid.a@gmail.com

This thesis was typed by the author.